

Best Available Copy

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-334511

(43)Date of publication of application : 22.11.2002

(51)Int.Cl. G11B 20/10
G06F 3/06
G06F 12/14
G11B 7/004
G11B 27/00

(21)Application number : 2002-022360 (71)Applicant : SONY COMPUTER ENTERTAINMENT INC
(22)Date of filing : 30.01.2002 (72)Inventor : KUTARAGI TAKESHI
OKAMOTO SHINICHI
MIURA KAZUO

(30)Priority

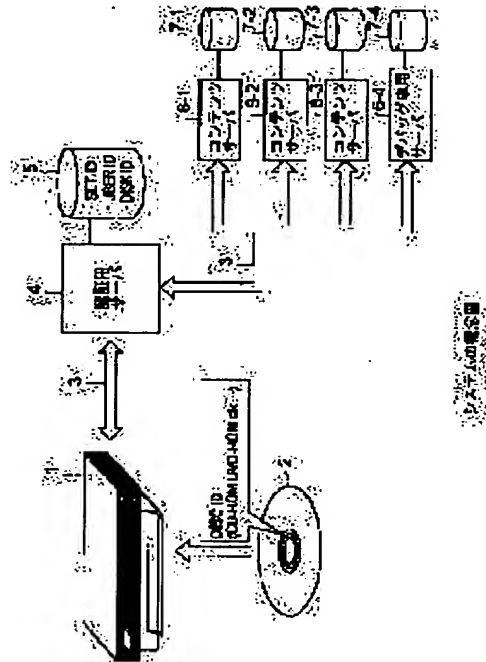
Priority number : 2001022811 Priority date : 31.01.2001 Priority country : JP

(54) COMPUTER SYSTEM AND ITS USING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a computer system having an authentication system which verifies whether an optical disk is illegally used or not.

SOLUTION: In the computer system, many computers to which optical disks can be loaded can be connected to an authenticating server through a network, and each computer has a peculiar device ID, and the server has a user database where the device ID is stored at the time of using the computer and a disk ID is stored at the time of using an optical disk, and data of a pair of the disk ID and the device ID is stored in the user database. When the optical disk is used at the second and following times, disk ID data and device ID data are transmitted to the authenticating server from the computer through the network to authenticate the normal use.



LEGAL STATUS

[Date of request for examination] 31.01.2002

[Date of sending the examiner's decision of rejection] 22.12.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

(19)日本国特許庁(JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開 2002-334511

(P2002-334511A)

(43)公開日 平成14年11月22日(2002.11.22)

(51)Int. Cl. ⁷	識別記号	F I	テ-マ-ド(参考)
G 1 1 B	20/10	G 1 1 B 20/10	D 5B017
			H 5B065
G 0 6 F	3/06	G 0 6 F 3/06	H 5D044
	12/14	3 0 4 12/14	F 5D090
G 1 1 B	7/004	G 1 1 B 7/004	C 5D110
審査請求	有	請求項の数 3 8	OL (全 1 8 頁) 最終頁に続く

(21)出願番号 特願2002-22360(P2002-22360)

(22)出願日 平成14年1月30日(2002.1.30)

(31)優先権主張番号 特願2001-22811(P2001-22811)

(32)優先日 平成13年1月31日(2001.1.31)

(33)優先権主張国 日本(JP)

(71)出願人 395015319

株式会社ソニー・コンピュータエンタテインメント

東京都港区赤坂7-1-1

(72)発明者 久多良木 健

東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

(74)代理人 100101867

弁理士 山本 寿武

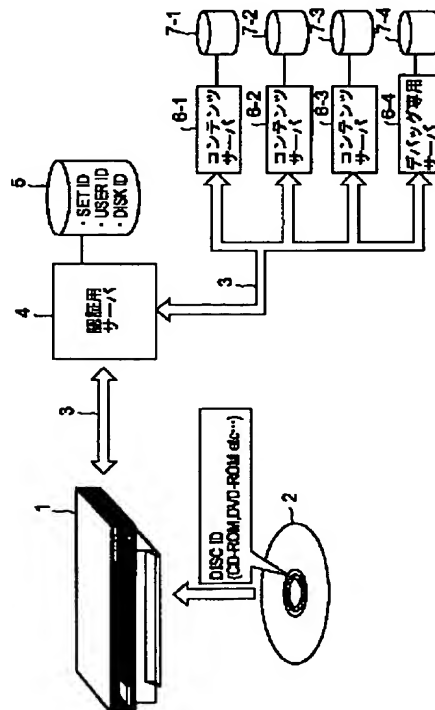
最終頁に続く

(54)【発明の名称】コンピュータシステム及びその使用方法

(57)【要約】

【課題】 光ディスクが不正使用されているか否かを検証する認証システムを有するコンピュータシステム

【解決手段】 光ディスクが夫々装着可能な複数のコンピュータがネットワークを介して認証用サーバに接続可能なコンピュータシステムであって、各々の前記コンピュータは固有の機器IDを有し、各々の前記光ディスクは固有のディスクIDを有し、前記サーバは、前記コンピュータの使用時に前記機器IDを、前記光ディスクの使用時にディスクIDを、夫々蓄積するユーザデータベースを有し、該ユーザデータベースにはディスクID-機器IDの組のデータが蓄積されており、前記光ディスクの2回目以降の使用時には、前記コンピュータから前記ネットワークを介してディスクIDデータと機器IDデータとを認証用サーバに送信し、正当な使用であることを認証する。



システムの概略図

【特許請求の範囲】

【請求項 1】 第 1 の記録媒体が装着される第 1 の情報処理装置と、

第 1 の情報処理装置とネットワークを介して接続される第 2 の情報処理装置とを備えたネットワークシステムにおいて、

第 2 の情報処理装置は、

第 1 の情報処理装置に関連した固有の情報と、第 1 の記録媒体に関連した固有の情報を前記第 1 の情報処理装置から受信し、

第 2 の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで記録媒体の認証を行う、ネットワークシステム。

【請求項 2】 請求項 1 に記載のネットワークシステムにおいて、該ネットワークシステムは、更に、第 2 の情報処理装置によって、第 1 の情報処理装置或いは第 1 の記録媒体に関連した固有の情報をデータベース内に蓄積する、ネットワークシステム。

【請求項 3】 請求項 1 に記載のネットワークシステムは、更に第 2 の情報処理装置によって、第 1 の情報処理装置及び第 1 の記録媒体に関連した固有の情報をデータベース内に蓄積する、ネットワークシステム。

【請求項 4】 請求項 1 ～ 3 のいずれか一項に記載のネットワークシステムにおいて、データベース内の情報は、予め記録された前記第 1 の情報処理装置或いは第 1 の記録媒体に関連した固有の情報である、ネットワークシステム。

【請求項 5】 請求項 1 ～ 3 のいずれか一項に記載のネットワークシステムにおいて、データベース内の情報は、予め記録された前記第 1 の情報処理装置及び第 1 の記録媒体に関連した固有の情報である、ネットワークシステム。

【請求項 6】 請求項 2 又は請求項 3 に記載のネットワークシステムにおいて、データベース内の情報は、あらたに蓄積された情報に更新される、ネットワークシステム。

【請求項 7】 請求項 2 ～ 6 のいずれか一項に記載のネットワークシステムにおいて、記録媒体が不正に使用された際に、第 1 の情報処理装置或いは第 1 の記録媒体に関連した固有の情報をデータベース内に蓄積する、ネットワークシステム。

【請求項 8】 請求項 1 ～ 7 のいずれか一項に記載のネットワークシステムは、更に第 2 の情報処理装置によって、第 1 の情報処理装置において実行される処理を可能あるいは不可能とする、ネットワークシステム。

【請求項 9】 請求項 1 ～ 8 のいずれか一項に記載のネットワークシステムは、更に第 2 の情報処理装置によって、第 1 の情報処理装置において実行される第 1 の記録媒体に記録されたプログラムの読取り処理を可能あるい

は不可能とする、ネットワークシステム。

【請求項 10】 請求項 8 又は請求項 9 に記載のネットワークシステムにおいて、

第 2 の情報処理装置は、第 1 の情報処理装置によって実行されるべき処理を可能とする許可信号、あるいは、第 1 の情報処理装置によって実行されるべき処理を不可能とする拒否信号を送信する、ネットワークシステム。

【請求項 11】 請求項 10 に記載のネットワークシステムにおいて、

第 2 の情報処理装置による参照の結果、データベース内に第 1 の記録媒体に関連した固有の情報に該当する情報が蓄積されている場合に、第 1 の情報処理装置によって実行される処理を可能とする、ネットワークシステム。

【請求項 12】 請求項 10 に記載のネットワークシステムにおいて、

データベース内には第 1 の情報処理装置に関連した固有の情報及び第 1 の記録媒体に関連した固有の情報とが関連付けられた情報として蓄積され、

第 2 の情報処理装置による参照の結果、第 2 の情報処理装置が受信した前記第 1 の情報処理装置に関連した固有の情報及び第 1 の記録媒体に関連した固有の情報が、データベース内の関連付けられた情報と一致した場合には、第 1 の情報処理装置によって実行される処理を可能とする、ネットワークシステム。

【請求項 13】 請求項 9 に記載のネットワークシステムにおいて、

第 1 の記録媒体にはプログラムが暗号化して記録され、第 2 の情報処理装置は、第 1 の情報処理装置によって暗号化された第 1 の記録媒体内のプログラムを解読するための情報を送信することで、第 1 の情報処理装置による第 1 の記録媒体の読取り処理を可能とする、ネットワークシステム。

【請求項 14】 請求項 13 に記載のネットワークシステムにおいて、

解読するための情報は、暗号解読用の鍵である、ネットワークシステム。

【請求項 15】 請求項 1 ～ 14 のいずれか一項に記載のネットワークシステムは、更に第 1 の記録媒体とは異なる第 2 の記録媒体が装着される第 3 の情報処理装置に接続され、

第 2 の情報処理装置によって、第 1 の情報処理装置から第 1 の記録媒体に関連する固有の情報を受信すると共に、第 3 の情報処理装置から第 2 の記録媒体に関連した固有の情報を受信する、ネットワークシステム。

【請求項 16】 請求項 15 に記載のネットワークシステムは、更に、

第 2 の情報処理装置によって、第 1 の情報処理装置から受信した第 1 の記録媒体に関連した固有の情報と、第 3 の情報処理装置から受信した第 2 の記録媒体に関連した固有の情報を参照し、参照した各固有の情報が重複し

た場合には、第3の情報処理装置において実行される第2の記録媒体に記録されたプログラムの読取り処理を可能あるいは不可能とする、ネットワークシステム。

【請求項17】 請求項16に記載のネットワークシステムは、更に第2の情報処理装置が、第1の情報処理装置に対して、第3の情報処理装置において行われる第2の記録媒体の実行処理を可能にするか否かに関して確認情報を送信する、ネットワークシステム。

【請求項18】 請求項17に記載のネットワークシステムにおいて第2の情報処理装置が、第1の情報処理装置から承諾が有った時、第3の情報処理装置において第2の記録媒体の実行処理を可能とする、ネットワークシステム。

【請求項19】 請求項1～18のいずれか一項に記載のネットワークシステムにおいて、第1の情報処理装置には更に第3の記録媒体が装着可能とされ、

第2の情報処理装置は、第1の情報処理装置から受信した第1の情報処理装置に関連した固有の情報及び第1の記録媒体に関連した固有の情報を受信した後に、各固有の情報を第1の情報処理装置に対して送信し、第1の情報処理装置は各固有の情報を、第2の記録媒体内に蓄積する、ネットワークシステム。

【請求項20】 請求項19に記載のネットワークシステムにおいて、更に第1の情報処理装置は、第1の記録媒体に関連した固有の情報と、第3の記録媒体内に蓄積された情報とを参照する、ネットワークシステム。

【請求項21】 請求項20に記載のネットワークシステムにおいて、第1の情報処理装置による参照の結果、第3の記録媒体内に第1の記録媒体に関連する固有の情報に該当する情報が蓄積されている場合には、第1の情報処理装置によって実行される処理を可能とする、ネットワークシステム。

【請求項22】 請求項1～21のいずれか一項に記載の前記ネットワークシステムにおいて、情報処理装置に関連した固有の情報は機器IDである、ネットワークシステム。

【請求項23】 請求項1～22のいずれか一項に記載の前記ネットワークシステムにおいて、情報処理装置に関連した固有の情報はユーザIDである、ネットワークシステム。

【請求項24】 請求項1～22のいずれか一項に記載の前記ネットワークシステムにおいて、前記記録媒体に関連した固有の情報は記録媒体IDである、ネットワークシステム。

【請求項25】 請求項1に記載のコンピュータシステムにおいて、前記アプリケーションを記録した記録媒体が光ディスクであり、前記記録媒体IDがディスクIDである、コン

ピュータシステム。

【請求項26】 請求項25に記載のコンピュータシステムにおいて、

前記ディスクIDは、前記光ディスクのデータエリア内の領域又はデータエリア以外の領域に記録されている、コンピュータシステム。

【請求項27】 請求項25に記載のコンピュータシステムにおいて、

前記コンピュータでは、前記ディスクIDは、前記光ディスクのデータエリアに記録されたディスクIDデータのアドレスに基づき検出される、コンピュータシステム。

【請求項28】 請求項25に記載のコンピュータシステムにおいて、

前記ディスクIDは、有機色素によりディスクに記録されている、コンピュータシステム。

【請求項29】 請求項25に記載のコンピュータシステムにおいて、

前記ディスクIDは、ビット列の物理的な変動を利用した方法で形成されている、コンピュータシステム。

【請求項30】 請求項29に記載のコンピュータシステムにおいて、

前記ビット列の物理的な変動を利用した方法は、ビット列の半径方向の変動、ビットサイズの短径方向の変動又はビットの深さ方向の変動のいずれかを利用している、コンピュータシステム。

【請求項31】 請求項25に記載のコンピュータシステムにおいて、

前記ディスクIDは、電子透かしを利用した方法で形成されている、コンピュータシステム。

【請求項32】 第1の記録媒体が装着される第1の情報処理装置、第1の情報処理装置とネットワークを介して接続される第2の情報処理装置を有するネットワークシステムを利用して、該記録媒体の認証を行う方法において、

第2の情報処理装置が、前記第1の情報処理装置から、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報を受信するステップと、第2の情報処理装置が、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む、方法。

【請求項33】 第1の記録媒体が装着される第1の情報処理装置であって、第2の情報処理装置とネットワークを介して接続された第1の情報処理装置において、該第1の情報処理装置は、

第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報を、前記第2の情報処理装置に送信し、

第2の情報処理装置に接続或いは含まれ、情報の蓄積・

10

20

30

40

50

消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第 1 の記録媒体の認証を行う、第 1 の情報処理装置。

【請求項 3 4】 第 1 の記録媒体が装着される第 1 の情報処理装置とネットワークを介して接続される第 2 の情報処理装置において、該第 2 の情報処理装置は、第 1 の情報処理装置に関連した固有の情報と、第 1 の記録媒体に関連した固有の情報とを前記第 1 の情報処理装置から受信し、
第 2 の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第 1 の記録媒体の認証を行う、第 2 の情報処理装置。

【請求項 3 5】 第 1 の記録媒体が装着される第 1 の情報処理装置とネットワークを介して接続される第 2 の情報処理装置で実行される、該第 2 の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体において、該プログラムは、
第 1 の情報処理装置に関連した固有の情報と、第 1 の記録媒体に関連した固有の情報とを前記第 1 の情報処理装置から受信するステップと、
第 2 の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第 1 の記録媒体の認証を行うステップとを含む、記録媒体。

【請求項 3 6】 第 1 の記録媒体が装着される第 1 の情報処理装置であって、第 2 の情報処理装置とネットワークを介して接続された第 1 の情報処理装置で実行される、該第 1 の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体において、該プログラムは、
第 1 の情報処理装置に関連した固有の情報と第 1 の記録媒体に関連した固有の情報とを、前記第 2 の情報処理装置に送信するステップと、
第 2 の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第 1 の記録媒体の認証を行うステップとを含む、記録媒体。

【請求項 3 7】 第 1 の記録媒体が装着される第 1 の情報処理装置とネットワークを介して接続される第 2 の情報処理装置で実行される、該第 2 の情報処理装置で読み取り可能且つ実行可能なプログラムにおいて、
第 1 の情報処理装置に関連した固有の情報と、第 1 の記録媒体に関連した固有の情報とを前記第 1 の情報処理装置から受信するステップと、
第 2 の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第 1 の記録媒体の認証を行うステップとを含む、プログラム。

【請求項 3 8】 第 1 の記録媒体が装着される第 1 の情

報処理装置であって、第 2 の情報処理装置とネットワークを介して接続された第 1 の情報処理装置で実行される、該第 1 の情報処理装置で読み取り可能且つ実行可能なプログラムにおいて、

第 1 の情報処理装置に関連した固有の情報と第 1 の記録媒体に関連した固有の情報とを、前記第 2 の情報処理装置に送信するステップと、

第 2 の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第 1 の記録媒体の認証を行うステップとを含む、プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムに関する。

【0002】

【従来の技術】光ディスクを装着して使用するコンピュータでは、各種のプログラムを実行することが出来る。このようなコンピュータの一つにエンタテインメントシステムがあり、代表的にはゲーム装置として使用されている。このようなエンタテインメントシステムでは、ゲームプログラムが記録された光ディスクを購入し、ゲームを実行する。また最近、エンタテインメントシステムは、ネットワークを介して、多数のゲームプログラムを蓄積したコンテンツサーバと接続され、ゲームプログラムをネットワークを介してダウンロードして購入するようなことも計画されている。

【0003】

【発明が解決しようとする課題】購入された光ディスク又はダウンロードしたプログラムを記録した光ディスクが、不正に使用される場合がある。即ち、プログラムを記録した光ディスクが、プログラムに関する著作権者の許可無く、不正にコピーされたり、これを中古品として販売されたりすることがある。このような状態を放置すると、著作権者は正当な利益を回収することが出来ず、プログラム創作の意欲が削がれることになる。

【0004】

【課題を解決するための手段】上述の問題点に鑑みて、本発明は、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムを提供することを目的とする。

【0005】更に、本発明は、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムの使用方法を提供することを目的とする。

【0006】本発明に係るネットワークシステムは、第 1 の記録媒体（例えば、光ディスク）が装着される第 1 の情報処理装置（例えば、一のエンタテインメント装置）と、第 1 の情報処理装置とネットワークを介して接続さ

れる第2の情報処理装置（例えば、認証用サーバ）とを備えたネットワークシステムであって、第2の情報処理装置は、第1の情報処理装置に関連した固有の情報（例えば、機器ID）と、第1の記録媒体に関連した固有の情報とを前記第1の情報処理装置から受信し、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで記録媒体の認証を行う。

【0007】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、該ネットワークシステムは、更に、第2の情報処理装置によって、第1の情報処理装置或いは第1の記録媒体に関連した固有の情報をデータベース内に蓄積する。

【0008】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第2の情報処理装置によって、第1の情報処理装置及び第1の記録媒体に関連した固有の情報をデータベース内に蓄積する。

【0009】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内の情報は、予め記録された前記第1の情報処理装置或いは第1の記録媒体に関連した固有の情報である。

【0010】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内の情報は、予め記録された前記第1の情報処理装置及び第1の記録媒体に関連した固有の情報である。

【0011】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内の情報は、あらたに蓄積された情報に更新される。

【0012】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、記録媒体が不正に使用された際に、第1の情報処理装置或いは第1の記録媒体に関連した固有の情報をデータベース内に蓄積する。

【0013】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第2の情報処理装置によって、第1の情報処理装置において実行される処理を可能あるいは不可能とする。

【0014】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第2の情報処理装置によって、第1の情報処理装置において実行される第1の記録媒体に記録されたプログラムの読取り処理を可能あるいは不可能とする。

【0015】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第2の情報処理装置は、第1の情報処理装置によって実行されるべき処理を可能とする許可信号、あるいは、第1の情報処理装置によって実行されるべき処理を不可能とする拒否信号を送信する。

【0016】更に、本発明に係るネットワークシステム

は、上述のネットワークシステムであって、第2の情報処理装置による参照の結果、データベース内に第1の記録媒体に関連した固有の情報に該当する情報が蓄積されている場合に、第1の情報処理装置によって実行される処理を可能とする。

【0017】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、データベース内には第1の情報処理装置に関連した固有の情報及び第1の記録媒体に関連した固有の情報とが関連付けられた情報として蓄積され、第2の情報処理装置による参照の結果、第2の情報処理装置が受信した前記第1の情報処理装置に関連した固有の情報及び第1の記録媒体に関連した固有の情報が、データベース内の関連付けられた情報と一致した場合には、第1の情報処理装置によって実行される処理を可能とする。

【0018】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第1の記録媒体にはプログラムが暗号化して記録され、第2の情報処理装置は、第1の情報処理装置によって暗号化された第1の記録媒体内のプログラムを解読するための情報を送信することで、第1の情報処理装置による第1の記録媒体の読取り処理を可能とする。

【0019】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、解読するための情報は、暗号解読用の鍵である。

【0020】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第1の記録媒体とは異なる第2の記録媒体（例えば、光ディスク）が装着される第3の情報処理装置（例えば、他のエンタテインメント装置）に接続され、第2の情報処理装置によって、第1の情報処理装置から第1の記録媒体に関連する固有の情報を受信した後に、第3の情報処理装置から第2の記録媒体に関連した固有の情報を受信する。

【0021】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第2の情報処理装置によって、第1の情報処理装置から受信した第1の記録媒体に関連した固有の情報と、第3の情報処理装置から受信した第2の記録媒体に関連した固有の情報とを参照し、参照した各固有の情報が重複した場合には、第3の情報処理装置において実行される第2の記録媒体に記録されたプログラムの読取り処理を可能あるいは不可能とする。

【0022】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第2の情報処理装置が、第1の情報処理装置に対して、第3の情報処理装置において行われる第2の記録媒体の実行処理を可能にするか否かに関して確認情報を送信する。

【0023】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第1の情報

処理装置から承諾があった時、第3の情報処理装置において第2の記録媒体の実行処理を可能とする。

【0024】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第1の情報処理装置には更に第3の記録媒体（例えば、メモリカード）が装着可能とされ、第2の情報処理装置は、第1の情報処理装置から受信した第1の情報処理装置に関連した固有の情報及び第1の記録媒体に関連した固有の情報を受信した後に、各固有の情報を第1の情報処理装置に対して送信し、第1の情報処理装置は各固有の情報を、第2の記録媒体内に蓄積する。

【0025】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、更に、第1の情報処理装置は、第1の記録媒体に関連した固有の情報と、第3の記録媒体内に蓄積された情報とを参照する。

【0026】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、第1の情報処理装置による参照の結果、第3の記録媒体内に第1の記録媒体に関連する固有の情報が該当する情報が蓄積されている場合には、第1の情報処理装置によって実行される処理を可能とする。

【0027】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、情報処理装置に関連した固有の情報は機器IDである。

【0028】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、情報処理装置に関連した固有の情報はユーザIDである。

【0029】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記記録媒体に関連した固有の情報は記録媒体IDである。

【0030】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記アプリケーションを記録した記録媒体が光ディスクであり、前記記録媒体IDがディスクIDである。

【0031】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクIDは、前記光ディスクのデータエリア内の領域又はデータエリア以外の領域に記録されている。

【0032】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記コンピュータでは、前記ディスクIDは、前記光ディスクのデータエリアに記録されたディスクIDデータのアドレスに基づき検出される。

【0033】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクIDは、有機色素によりディスクに記録されている。

【0034】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクIDは、ビット列の物理的な変動を利用した方法で形

成されている。

【0035】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ビット列の物理的な変動を利用した方法は、ビット列の半径方向の変動、ビットサイズの短径方向の変動又はビットの深さ方向の変動のいずれかを利用している。

【0036】更に、本発明に係るネットワークシステムは、上述のネットワークシステムであって、前記ディスクIDは、電子透かしを利用した方法で形成されている。

【0037】更に、本発明に係る記録媒体の認証を行う方法は、第1の記録媒体が装着される第1の情報処理装置、第1の情報処理装置とネットワークを介して接続される第2の情報処理装置を有するネットワークシステムを利用して、該記録媒体の認証を行う方法であって、第2の情報処理装置が、前記第1の情報処理装置から、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報を受信するステップと、第2の情報処理装置が、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで記録媒体の認証を行うステップとを含む。

【0038】更に、本発明に係る第1の情報処理装置は、第1の記録媒体が装着される第1の情報処理装置であり、第2の情報処理装置とネットワークを介して接続された第1の情報処理装置であって、該第1の情報処理装置は、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報を、前記第2の情報処理装置に送信し、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第1の記録媒体の認証を行う。

【0039】更に、本発明に係る第2の情報処理装置は、第1の記録媒体が装着される第1の情報処理装置とネットワークを介して接続される第2の情報処理装置であって、該第2の情報処理装置は、第1の情報処理装置に関連した固有の情報と、第1の記録媒体に関連した固有の情報を前記第1の情報処理装置から受信し、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行う。

【0040】更に、本発明に係る記録媒体は、第1の記録媒体が装着される第1の情報処理装置とネットワークを介して接続される第2の情報処理装置で実行される、該第2の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体であって、該プログラムは、第1の情報処理装置に関連した固有の情報と、第1の記録媒体に関連した固有の情報を前記第1の情報処理装置から受信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータ

ベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む。

【0041】更に、本発明に係るプログラムは、第1の記録媒体が装着される第1の情報処理装置であって、第2の情報処理装置とネットワークを介して接続された第1の情報処理装置で実行される、該第1の情報処理装置で読み取り可能且つ実行可能なプログラムを記録した記録媒体であって、該プログラムは、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報とを、前記第2の情報処理装置に送信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む。

【0042】更に、本発明に係るプログラムは、第1の記録媒体が装着される第1の情報処理装置とネットワークを介して接続される第2の情報処理装置で実行される、該第2の情報処理装置で読み取り可能且つ実行可能なプログラムであって、該プログラムは、第1の情報処理装置に関連した固有の情報と、第1の記録媒体に関連した固有の情報とを前記第1の情報処理装置から受信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、受信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む。

【0043】更に、本発明に係るプログラムは、第1の記録媒体が装着される第1の情報処理装置であって、第2の情報処理装置とネットワークを介して接続された第1の情報処理装置で実行される、該第1の情報処理装置で読み取り可能且つ実行可能なプログラムであって、該プログラムは、第1の情報処理装置に関連した固有の情報と第1の記録媒体に関連した固有の情報とを、前記第2の情報処理装置に送信するステップと、第2の情報処理装置に接続或いは含まれ、情報の蓄積・消去等が可能なデータベース内の情報と、送信した固有の各情報とを参照することで第1の記録媒体の認証を行うステップとを含む。

【0044】

【発明の実施の形態】以下、添付の図面を参照しながら本実施形態について詳細に説明する。

〔ディスク認証システム〕

（システム全体）図1は、本実施例に係るディスク認証システム全体の概念図である。図1に示されるように、ユーザ端末機器1が、ネットワーク3を介して認証用サーバ4と接続されている。この認証用サーバ4は、ネットワーク3を介して1又は2以上のコンテンツサーバ6と接続されている。これらのコンテンツサーバ6にはデバッグ専用サーバ6-4があってもよい。

【0045】ユーザ端末機器1は、アプリケーションプログラムを記録したCD-ROM (Compact Disc-Read

Only Memory)、DVD-ROM (Digital Versatile Disc-ROM) 等の光ディスク2を搭載可能なコンピュータである。本実施例では、ゲーム機等に代表されるエンタテインメントシステムを例にとって説明する。このユーザ端末機器1はエンタテインメント本体装置に該当し、エンタテインメント本体装置に関しては、後で図2を用いてその内部の構成を説明する。なお、光ディスク2は、例示であって、これに限定されない。アプリケーションプログラム等のコンテンツを記録した種々の記録媒体全てが対象となることを承知されたい。例えば、外部接続のハードディスク（図示せず。）、後述のコネクタに接続されるメモリカード又はPDA内のメモリ等にアプリケーションプログラム等のコンテンツが記録されている場合には、これらは対象となる。しかし、説明を分かり易くするため、光ディスク2を例にとって説明する。

【0046】ネットワーク3としては、テレビジョンケーブルネットワーク、光ファイバネットワーク、xDSL (x Digital Subscriber Line) 等のいわゆるブロードバンドネットワークが好ましい。また、既存の又はこれから構築される広帯域無線ネットワーク、携帯電話及びPHS (Personal Handyphone System) 電話関連のネットワーク、インターネット関連のネットワーク等も利用することができる。

【0047】認証用サーバ4は、エンタテインメント装置1に接続され、エンタテインメント装置1及び記録媒体2が真正であるか不正であるかの認証を行うために用いられるサーバである。認証用サーバ4は、各々のエンタテインメント本体装置1に付与された固有のIDである機器ID (「SET ID」とも言う。) 情報と、各々のユーザに付与された固有のIDであるユーザID (「USER ID」とも言う。) 情報 (パスワードを含む場合もある。) と、各々の光ディスク2に付与された固有のIDであるディスクID (「DISK ID」とも言う。) 等のユーザ情報を蓄積するユーザデータベース5を有する。これらのIDは、各々単一のものであり、同じIDは2つ以上存在しない。特に、ディスクIDは、光ディスク1枚毎に付された相異なる識別記号である。

【0048】また、コンテンツサーバ6は、ユーザに提供し得る種々のデジタルコンテンツを蓄積したデータベース7を夫々有している。

【0049】更に、認証用サーバ4の代わりに、エンタテインメント装置1を用いることもできる。即ち、複数のエンタテインメント装置1が接続されて、その内の特定の一台が認証用サーバの役割を果たす場合である。この場合、これに接続されるユーザデータベース5は、ハードディスクのような記録媒体で構成される。

【0050】（装置本体の内部構成）図2は、図1のユーザ端末として利用されるエンタテインメントシステム

の本体装置の内部構成のブロック図である。図中、一点鎖線内はエンタテインメント本体装置1を、破線内は該エンタテインメント本体装置1のディスクドライブ30を、夫々示している。

【0051】エンタテインメント本体装置1はCPU16を有し、このCPU16はメインメモリ(RAM)17と接続されている。また、CPU16は描画装置(GPU)18と接続されており、GPU18からの映像信号は、CRT-CTR(Cathode Ray Tube-Control)

(図示せず。)を介して表示装置(CRT)(図示せず。)に出力されている。また、CPU16は、USB(Universal Serial Bus)コネクタ14、IEEE1394又はiリンク(i.LINK(登録商標))コネクタ15等を有するIOP(Input/Output Processor)13を介して、コネクタ(コントローラ(PAD)/PDA(Personal Digital Assistant)/メモリカード・コネクタ)12に接続されている。

【0052】このコネクタ12には、メモリカード11、コントローラ(PAD)10、携帯端末(PDA: Personal Digital Assistant)等が接続される。このメモリカード11、PDA等は、外部記憶装置の一種であり、後述するように、ディスクID、機器ID等が記録される。

【0053】また、CPU16は、IOP13を介してバス27に接続され、このバス27には、MASK-ROM(Masked ROM)19、CD/DVD-DSP(CD/DVD-Digital Signal Processor)22、DVDプレイヤーROM20、SPU(Sound Processing Unit)25、ネットワーク・インターフェース26等が接続されている。SPU25からの音声信号は、アンプ、スピーカ等(図示せず。)に出力されている。エンタテインメント本体装置1は、ネットワーク・インターフェース26、USBコネクタ14、iリンクコネクタ15等を介してネットワークと接続され、更にネットワークを通じて認証用サーバ4、デジタルコンテンツサーバ6等に接続される。

【0054】CD/DVD-DSP22は、メカニカル制御部23及びドライバ24を介して、ディスクドライブ30の機械的制御を行う。この制御は、RF-AMP(Radio Frequency Amplifier)21を通じて行われる。また、CD/DVD-DSP22は、RF-AMP21を通じて、ディスクドライブ30の電氣的制御を行う。

【0055】光ディスク2は、スピンドルモータ(図示せず。)の機械的制御により回転される。また、光ディスク2に対しては、アクチュエータ(図示せず。)の電氣的制御によりピックアップレンズ(図示せず。)が駆動されて情報の記録/再生が行われる。

【0056】このエンタテインメント装置1は、製造番号等の固有のIDである機器IDを有している。この機

器IDは、例えば予めマスクROM19に書き込まれるようにハードウェア的に組み込まれたもの、或いは後から光ディスク2、メモリカード11、携帯端末、コントローラ10等を介してソフトウェア的に読み込まれたものの、のいずれでもよい。

【0057】また、この光ディスク2にはディスクIDが記録されており、このディスクIDは後述する方法で読み取られる。

[ディスクID認証システム]

(第1のディスクID認証システム)以下、図3を用いて第1のディスクID認証システムのエンタテインメント本体装置側の処理に関して具体的に説明し、図4を用いて認証用サーバ4側の処理に関して具体的に説明する。なお、本実施例においては、エンタテインメントシステムはゲーム機であり、ゲームプログラムを記憶した記録媒体としてはCD-ROMのような光ディスクを使用し、更にディスクIDが通常のデータエリア以外のエリア(例えば、リードインエリアの内側、リードアウトの外側等)に存在する場合を前提として説明する。

【0058】図3は、エンタテインメント本体装置側の処理を示している。まず、エンタテインメント本体装置における処理の基本を説明する。ここで使用されている光ディスクは、通常では記録対象となっていないエリアにディスクIDが記録されている。このディスクIDの記録箇所を特定する情報(例えば、アドレス)は、通常のデータエリアに記録されている。光ディスク2にディスクIDを記入するための材料としては、追記型ディスクに使用されている有機色素が一例として挙げられる。エンタテインメント本体装置は、ディスク情報を読み取り、そこからディスクIDの記録されたアドレスを検索し、更にこのアドレスに従ってディスクIDを読み取り、それを認証用サーバ4に送信している。以下、具体的に説明する。

【0059】ステップS102において、エンタテインメント本体装置1は、CPUの制御のもと、搭載されたCD-ROMからTOC(Table of Contents)の基礎データを読み込む。そして、ステップS103において、CD-ROMのデータエリアのボリューム識別子VD(Volume Description)を読み込み、ディスクIDの記入してあるアドレスを検索する。

【0060】ステップS104では、ボリューム識別子VDにディスクIDのアドレスが存在するか否かが判定される。IDのアドレスが存在しなければ、搭載されたCD-ROMは、このディスクID認証システムによる保護対象以外のCD-ROMと判定され、ステップS113に進行し、プログラムが実行される。このエンタテインメント本体装置1は、単にゲーム機として機能するだけでなく、音楽用CD再生装置、映画用DVD再生装置等としても機能する。このため、エンタテインメント本体装置に、ID認証システムによる保護対象以外の光ディスク

(例えば、DVD-Video、Audio-CD、従来のゲームCD等)が搭載されている場合があり、このような場合はそのまま音楽や映像の再生やゲームの実行が行われる。

【0061】ボリューム識別子VDにIDアドレスが存在する場合、ステップS105において、ディスクIDを読み取るために、IDアドレスに従って光ディスクドライブ30のピックアップをCD-ROMのディスクIDデータ部(リードインエリア内側又はリードアウトの外側に設けられた部分)に向けてスライドさせる。このピックアップのスライド制御は、CPU16から出力されたスライド命令に基づいて、メカニカル制御部23にて行われる。

【0062】ステップS106において、CPU16は、CD-ROM上のディスクIDデータ部に、実際にディスクID情報が存在するか否かを判別する。ディスクID情報が存在しない場合又はディスクID情報の読み込みが不可能な場合には、ディスクID無しと判定され、ステップS107に進む。このステップS107では、プログラムの実行は拒否され、強制終了される。

【0063】ディスクIDデータ部に実際にディスクID情報が存在する場合、エンタテインメント本体装置1は、ステップS108において、CPUの制御の下、ディスクID情報を読み取りこれをメインメモリ17に記憶する。

【0064】ステップS109において、エンタテインメント本体装置1のCPU16は、ディスクIDのデータを、USB、IEEE(Institute of Electrical and Electronic Engineers)1394、PCMCIA(Personal Computer Memory Card International Architecture)等の規格に準拠した各種通信インターフェイスを介して、認証用サーバ4に対して送信する。そして、ステップS110で、送信したディスクIDに対して認証用サーバが認証処理を行うのを待つ。

【0065】ステップS111において、エンタテインメント本体装置1は、認証用サーバでの認証処理結果を受信する。認証用サーバでの認証処理の結果が「認証適」であれば、CD-ROMの読み取り許可命令が受信される。認証処理の結果が「認証否」であればステップS112に進み、プログラムの実行が拒否されて強制終了される。

【0066】認証用サーバでの認証処理の結果が「認証適」の場合、ステップS113において、エンタテインメント本体装置1のCPUは、CD-ROMに記録されたプログラムを実行する。

【0067】図4は、第1のディスクID認証システムにおける認証用サーバ4側の処理を示している。まず、認証用サーバ4における処理の基本を説明する。エンタテインメント本体装置1を購入したユーザは、その直後に、自分の氏名等のユーザIDと、各本体機器に付与さ

れた機器IDとを認証用サーバ4のユーザデータベース5に登録している。また、新たなゲームプログラムを購入したユーザは、その最初の使用時にディスクID情報を認証用サーバ4のユーザデータベース5に送信しなければ、そのプログラムの実行が出来ない(ステップS109参照)。このため、認証用サーバ4のユーザデータベース5には、ユーザ情報として、少なくともディスクIDと、更に、これと関連するユーザID、機器ID等の任意のものが蓄積される。ユーザ情報は、ユーザが複数の種類のゲームプログラムを購入すると、1つのユーザID及び機器IDに対して複数のディスクIDの組み合わせとなる。ユーザ情報は、テーブル化されてユーザデータベース5に蓄積される。

【0068】このような状況下で、ユーザがゲームを開始する場合、ユーザが使用しているディスクIDと機器IDの情報が、エンタテインメント本体機器1から認証用サーバ4に送信され、認証用サーバ4のユーザデータベースに蓄積されたユーザ情報と比較される。この比較結果は、図7に示すように、次の4通りとなる。

【0069】(No.1)ディスクIDと機器IDの両方が、蓄積されたものと一致する。

【0070】(No.2)ディスクIDのみが、蓄積されたものと一致する。

【0071】(No.3)機器IDのみが、蓄積されたものと一致する。

【0072】(No.4)ディスクIDと機器IDのいずれも、蓄積されたものとは一致しない。

【0073】No.1の、送信されたディスクIDと機器IDの組み合わせが、既にユーザデータベースに登録されたこれらに対応する情報と一致した場合、このディスクは正規のディスクと判断される。しかし、希なケースとして、機器IDが不正にコピーされ、且つディスクIDも不正にコピーされたような場合が起こる可能性がある。このようなケースを排除するため、同一のディスクIDと機器IDの組み合わせの認証要求が、同じ時間帯に重複した場合は不正使用であると判断し、この不正使用をカウントしてユーザデータベース5に記録すると共に、プログラムの実行を拒否する。

【0074】No.2の、送信されたディスクIDと機器IDの組み合わせの内、ディスクIDのみがデータベースに蓄積されたものと一致した場合、次の3通りの状況が考えられる。

【0075】(1)ディスク所有者が自分のディスクを他人に貸与した場合

(2)ディスク所有者が自分のディスクを他人の機器で実行した場合

(3)不正コピーの場合

これらのいずれに該当するかは、ディスクIDと共に登録されている機器IDのユーザに確認を求めることにより、判別できる。このエンタテインメントシステムは、

各エンタテインメント本体装置1が認証用サーバ4に対して接続されていることにより、このような確認作業が可能となる。

【0076】No. 3及びNo. 4の、送信されたディスクIDと機器IDの組み合わせの内、ディスクIDが未登録の場合、ディスク2の初回使用と判断され、ユーザデータベース5にディスクIDが登録される。以下具体的に説明する。

【0077】ステップS202において、認証用サーバ4は、ユーザが使用するエンタテインメント本体装置1に対する接続認証を行う。ここで、本体装置1の機器IDが、本体装置1からの送信データの一部として自動的にサーバに供給されるなら、ユーザはユーザIDであるパスワードのみを入力すればよい。接続認証に失敗した場合、ステップS203において、ユーザ端末装置と認証用サーバ4の間の接続は遮断される。接続認証が成功すれば、ステップS204において、ユーザの本体装置1との通信接続が確立される。

【0078】ステップS205において、認証用サーバ4は、エンタテインメント本体装置1からディスクIDデータ及び機器IDを受信する。これは図3のステップS109に対応する処理である。

【0079】ステップS206において、認証用サーバ4は、受信したディスクID、機器IDと、ユーザデータベース5に記録されているユーザ情報（ディスクID、機器ID）との比較を行う。

【0080】ステップS207において、受信したディスクIDが、データベース5に登録されたディスクIDと一致しているか否かが判定される。即ち、受信したディスクIDが、ユーザデータベース5上のテーブルになれば、そのディスクは初回の使用である。この場合はステップS208に進み、認証用サーバ4は、データベース5へのディスクIDの登録を行う。そして、ステップS212で、プログラム実行許可命令をエンタテインメント本体装置1に送信する。

【0081】送信ディスクIDがデータベース5に登録済みであれば、ステップS209に進み、受信機器IDと、前記ディスクIDの使用機器として登録された機器IDとが一致しているか否かが判断される。機器IDが不一致の場合、ステップS210に進み、ディスクIDに対応する機器IDのユーザ（ディスク所有者）に対して、使用許可の確認をする。ステップS211で、ディスク所有者が承諾すれば（即ち、ディスク所有者が、ディスク使用を承諾する旨をサーバ4に返信すれば）、これはディスク所有者が自分のディスクを他人に貸与したか、他のエンタテインメント本体装置1を利用して実行しているかであり、ステップS212で、プログラム実行許可命令をエンタテインメント本体装置1に送信する。

【0082】ディスク所有者が承諾しない場合、不正使用と判断され、ステップS214で不正使用のカウントがな

され、ステップS215で、プログラム実行拒否命令がエンタテインメント本体装置に送信される。これにより、中古品等の不正使用が排除される。

【0083】ディスクIDと機器IDの組み合わせがユーザデータベース5に登録されているユーザ情報と一致していた場合でも、極めて希なケースであるが両方のIDが不正にコピーされた場合には、これを排除する必要がある。ステップS213で、同じ時間帯に同じディスクID－機器IDの組み合わせでの使用が重複しているか否かが判断される。同時使用が発生していない場合、ステップS212で、プログラム実行許可命令がエンタテインメント本体装置1に送信される。同時使用が発生している場合、不正使用と判断され、ステップS214で不正使用のカウントがなされ、ステップS215で、プログラム実行拒否命令がエンタテインメント本体装置に送信される。

【0084】通常、不正ディスクは真正なディスク内容をそのままコピーするため、データエリアに記録されたディスクIDのアドレスデータもコピーされてしまう。しかし、本実施の形態のフォーマットにおける、リードインエリアの内側又はリードアウトエリアの外側等のデータエリア以外に記録されたID情報は、真正ディスクをそのままコピーした不正ディスクにはコピーされない。これにより、不正ディスクにはディスクIDのアドレスに関する情報はコピーされているにもかかわらず、ディスクID自体が存在しないので、不正ディスクに対しては、図3のステップS104でディスクIDのアドレス有りと判定され、次いでステップS106でディスクID自体なしと判定されることにより、ステップS107でプログラムの実行が排除されることとなる。

【0085】ディスクIDの記録方法は、上述の方法に限定されない。例えば、ディスクIDは、データエリア内に、ビット列の物理的な変動を利用した方法で形成することも出来る。このビット列の物理的な変動を利用した方法は、ビット列の半径方向の変動（ウォブリング）、ビットサイズの短径方向の変動又はビットの深さ方向の変動のいずれかを利用することが出来る。或いは、ディスクIDは、電子透かし(Digital Watermark)を利用した方法で形成することも出来る。

【0086】認証用サーバへのディスクIDの登録方法は、上述の方法に限定されない。なお、特別な場合として、例えば光ディスク等の記録媒体の提供者自身が認証用サーバ4を提供するような場合がある。この場合には、自ら製造・提供するディスクIDは、予め認証用サーバ4のデータベース5に登録・蓄積しておくことが出来る。このような場合、第1のディスクID認証システムでは、初回使用時のディスクIDの登録処理は不要となる。

【0087】また、機器IDは必ずしも必要でない。機器IDは各々のユーザ固有のユーザIDで置き換えることが出来る。即ち、使用機器を特定する代わりに、ユー

10

20

30

40

50

ザを特定し、ユーザIDとディスクIDとの組み合わせにより、認証システムを機能させることが出来る。この場合、好ましくは、ユーザIDはパスワードの形式で付与される。

【0088】光ディスク等の記録媒体の提供者自身が認証用サーバ4を提供するような場合について、更に説明する。

【0089】この記録媒体提供者が、ディスク製造時に、ディスク一枚毎に個別の製造番号を与え、これをディスクIDとしてディスク2内に情報として組み込む。同時に、ユーザデータベース5には、そのディスクID（製造番号）が記録されている。一方で、エンタテインメント装置1の製造時に、エンタテインメント装置一台毎に個別の製造番号を与え、これをエンタテインメント装置内に機器IDとして組み込まれている。そして同時に、ユーザデータベース5には、その機器ID（製造番号）が記録されている。

【0090】この場合、ディスク2の工場出荷時には、ディスクIDは、エンタテインメント装置1の機器IDと未だ関連付けられていない。

【0091】ディスク2の利用者が、認証用サーバ4に対して接続・認証処理の要求を行う（S109）と、認証用サーバ4は機器ID認証後に、ディスクIDの認証を行う。

【0092】ユーザデータベース5には、予め機器ID、ディスクID（ユーザ情報）が記録されているので、認証用サーバ4はエンタテインメント装置1から受信した機器ID-ディスクIDがこのユーザデータベース5に記録されたユーザ情報に該当するか否かをチェックする。

【0093】その結果、ユーザデータベース5のユーザ情報に該当するものがなかった場合には、認証を強制終了してディスク2のプログラム実行を拒否する。この際、不正なディスクIDをユーザデータベース5に蓄積するようにしておけば、各エンタテインメント装置毎の不正なディスクを利用しての認証用サーバ4へのアクセス回数のカウントや、不正ディスクを利用したエンタテインメント装置1の特定等の不正ディスクに関わる管理が可能となる。

【0094】また、不正なディスクの排除以外に関しても、ディスクIDが付与されたディスク2を用いたアクセス回数のカウントは、本発明のネットワークシステムにおいて有効に利用することが可能である。即ち、認証用サーバ4へのアクセス回数を利用して、アクセス回数がある回数以上に達した時、認証を強制終了してディスク2のプログラム実行を拒否するようにすることも出来る。

【0095】例えば、IDが付与されたディスク2を用いた認証用サーバ4へのアクセス回数を管理することで、ディスク2に含まれるプログラム等のコンテンツに

対しお試し期間を設けてユーザに利用させることが可能である。これにより、ユーザはあるディスク2の利用回数がある一定回数に達するまでは、お試し期間としてディスク内のプログラム等のコンテンツを利用してゲームやサービス等を利用することが可能である。

【0096】現在、多くのインターネット接続サービス体験版ソフトは、利用時間をカウントすることでお試し期間を設けているが、本発明のネットワークシステムを用いれば、サービスの利用時間による管理ではなく利用回数による管理が可能となる。

【0097】例えば、音楽や映像を、本発明の認証用サーバ4を介してコンテンツサーバ6からエンタテインメント装置1に対してダウンロード提供するサービスに利用可能である。ここで、サービスに加入したユーザは、サービス提供者からサービス利用のためのディスク2を配布されるものとする。ディスク内には、ディスク毎に付与されたディスクIDと共に、認証用プログラム、ダウンロード実行用プログラム等が記録されている。ユーザは、このディスク2をエンタテインメント装置1に装着することで認証用サーバ4並びにコンテンツサーバ6に接続することが可能となり、これにより音楽や映像等をダウンロード可能となる。

【0098】この際、ダウンロード回数をディスクIDを付与したディスク2を用いたコンテンツサーバ6へのアクセス回数として認証用サーバ4がカウントすれば、ダウンロード（通信）時間に依存しない、サービスの利用回数制限が実現可能となる。

【0099】更に、認証用サーバ4においてユーザがアクセスしたコンテンツ内容を表す情報とユーザ情報（機器ID、ユーザID、ディスクID等）とを相互に関連付けてユーザデータベース5内に蓄積していけば、ユーザ毎の嗜好等を容易に管理することが可能となる。これらの蓄積情報を用いて、サービス提供者或いはコンテンツ提供者は各ユーザ毎に適切な広告等をインターネット等の通信回線を通じて提供することが可能となる。

【0100】以上は利用回数に応じた、サービス提供等の利用制限方法であったが、制限方法はこれに限られない。例えば、ディスクIDが付与されたディスク2に記録された内容を、サービス提供者がユーザからの徴金状況に応じて、制限を付けて提供することもできる。ディスク2に記録された内容は、すべてを利用可能ではなく部分的に利用可能であるとする。ユーザが、その部分的に利用ができない内容を利用したい時には、ユーザはその利用内容に応じた対価をサービス提供者に支払うこととなる。サービス提供者は、それを受けて、ユーザによる利用を可能とする。

【0101】例えば、ディスク2に記録された内容を部分的に暗号化しておけば、利用対価を支払わないユーザは暗号部分に相当する利用できないが、利用対価を支払ったユーザに対しては、暗号を解読するための鍵をサー

ビス提供者からユーザのエンタテインメント装置1に提供を行うことで、利用可能となる。前記サービス提供者からエンタテインメント装置1に対して送信される情報は、暗号解読用の鍵には限られない。

【0102】また、ユーザがディスク2の部分的に利用できない記録内容を利用するためにサービス提供者に対して行うのは、対価の支払いに限られず、例えばユーザのエンタテインメント装置1からサービス提供者が運営する認証用サーバ4への、ユーザIDの送信であってもよい。このユーザIDは、サービス提供者から各ユーザに対して予め付与されたIDであってもよい。

【0103】(第2のディスクID認証システム) 次に、第2のディスクID認証システムについて説明する。第2のディスクID認証システムでは、認証対象となるディスクは、CD-ROM等に限定されず、TOCの規定されていないDVD-ROM等も含められる。また、ディスク内のディスクIDの記録箇所も限定されておらず、リードインエリアの内側、リードアウトの外側、又はデータエリア内のいずれの箇所であってもよい。

【0104】上記第1のディスク認証システムと比較すると、第1のディスク認証システムでは、ゲームをプレーするためにディスク上のプログラムを起動する毎に、サーバに接続して認証を行っていたが、この第2のディスク認証システムでは、ユーザ情報をメモリカード11等の本体接続型の外部記憶装置に記憶することで、サーバに接続する処理行程を省略している。即ち、ディスクの初回使用時に、メモリカード11等にディスクID-機器IDのユーザ情報を記録し、ゲーム実行毎にこのユーザ情報を利用してディスクの認証を行っている。なお、外部記憶装置には、アプリケーションプログラム等のコンテンツが記録されていてもよい。

【0105】図5を用いて第2のディスクID認証システムのエンタテインメント本体装置側の処理について具体的に説明し、図6を用いて認証用サーバ4側の各ステップでの処理内容について具体的に説明する。

【0106】ステップS302で、エンタテインメント本体装置1は、CPU16の制御の下、装着ディスク2に記録されている固有の基礎データをメインメモリ17に読込む。装着ディスク2は、CD、CD-ROM、DVD-Video、DVD-ROM等の各種ディスクが含まれる。

【0107】ステップS303では、読み込んだ基礎データの中にディスクIDが有るか否かが判断される。ディスクIDが存在しなければ、認証対象以外のディスクであると判断され、ステップS312に進み、プログラムが実行される。

【0108】ディスクIDが存在する場合、ステップS304に進み、CPU16の制御の下、エンタテインメント本体装置に接続されたメモリカード11等の外部記憶装置に記録されたユーザ情報(ディスクID-機器IDの

組み合わせデータ)が読み込まれる。なお、このメモリカード11等には、ゲームのハイスコア、前回中断したゲームの進行状況のバックアップデータ等のデータも記録されている。

【0109】ステップS305では、メモリカード11にディスクIDが記録されているか否かが判断される。ディスクを最初に使用した時に、メモリカード11のユーザ情報にディスクIDと機器IDとが登録されるため、2回目以降の使用時には、メモリカード11に、ディスクIDがユーザ情報として記録されていることになる。従って、メモリカード11にディスクIDの記録が無い場合としては、①ディスクの初回使用時、②メモリカード自体の交換時、等が考えられる。読み取ったディスクIDがメモリカード等に記録されていた場合、ステップS306に進む。

【0110】ステップS306では、メモリカード11等に記録されているディスクIDが、装着ディスクのディスクIDと一致するか否かが判断される。一致しない場合としては、ディスクの初回使用時その他が考えられる。一致していれば、ステップS307に進む。

【0111】ステップS307において、メモリカード11から読み込んだ機器IDが、現在使用している本体装置の機器IDと一致するか否かが判断される。一致しない場合としては、ディスク所有者からディスク2とメモリカード11とを借りてきたユーザが、自らの本体装置でゲームをする場合等が考えられる。一致する場合(ディスクID-機器IDの組み合わせが、ディスク購入時にメモリカード等に記録したユーザ情報と一致している場合)、正当使用に該当し、ユーザ認証を完了して、ステップS312でプログラムが実行される。

【0112】ステップS305で、メモリカードにディスクIDが存在しなかった場合、ステップS306で、メモリカード11等に記録されているディスクIDがディスクから読み込んだディスクIDと一致しなかった場合、又はステップS307で、メモリカード11等に記録されている機器IDが使用機器の機器IDと一致しなかった場合は、ステップS308に進む。このステップS308で、エンタテインメント本体装置は、USB、IEEE1394、PCMCIA等の通信インターフェイスを介して、ディスクID、使用機器の機器IDデータを認証用サーバ4に対して送信し、ステップS309でユーザ認証を待つ。この後、認証用サーバ4から、これらのディスクID、機器IDデータをメモリカード11に記録する命令を受信したときは、これらの書き込みを行う(図6のステップS405に対応)。

【0113】ステップS310で、認証用サーバ4での認証処理結果を元にプログラムの実行の可否を決定する。

「認証否」の場合、ステップS311に進み、プログラムの実行が拒否され、強制終了される。「認証適」の場合、ステップS312に進み、プログラムを実行する。

【0114】図6は、第2のディスクID認証システムにおける認証用サーバ4側の処理内容を示している。

【0115】ステップS402で、認証用サーバ4は、エンタテインメント本体装置に対する接続を確立した後、ディスクID、本体装置の機器IDを受信する。ディスクIDは、図5のステップS302でディスクから読み取られ、ステップS308で送信されたディスクIDであり、機器IDもステップS308で送信されたものである。

【0116】ステップS403で、受信したディスクIDが認証用サーバ4のユーザデータベースに蓄積されているディスクIDの中に存在するか否かが判定される。存在しない場合、そのディスクは初回使用と判断される。従って、ステップS404で、受信したディスクID－機器IDの組み合わせが、ユーザデータベース5にユーザ情報としてテーブル化して蓄積（登録）される。次いで、ステップS405で、ディスクID－機器IDを互に関連付けてユーザの本体装置1に接続されているメモリカード11等に記録させることで、図5で説明した認証処理を可能とする。

【0117】ステップS406で、認証用サーバ4は、使用ディスクに対するパスワードを本体装置1に送信する。このパスワードは、ディスクの所有者しか知り得ない秘密キーであり、後述するように、ユーザの意思確認のために使用される。このパスワードは、ユーザが使用する本体装置1の画面に対して出力されることが好ましい。ユーザはこのパスワードを書き留めておくことにより、他人へディスクを貸出すときにパスワードを教え、その他人がディスクを使用できるようにすることが可能となる。その後、ステップS414で、エンタテインメント本体装置に対してプログラム実行許可命令を送信する。

【0118】ステップS403で、受信ディスクIDが、登録されているディスクIDと一致した場合、ステップS407で、受信した機器IDが、前記ディスクIDに対応するデータベース中の機器IDと一致するか否かが比較され、ステップS408で、両者が一致するか否かが判定される。一度でも使用されたディスクに関しては、ユーザデータベース5にディスクID－機器IDの組み合わせからなるデータが蓄積されているため、このステップS408においては、機器IDがディスクIDに対応するものであるか否かを判別する。これにより、中古使用を排除することが出来る。メモリカード11の交換、メモリカードのディスクID－機器IDの記録の消失等の場合、ステップS409で、認証用サーバ4は、ディスクID－機器IDの組み合わせデータをエンタテインメント本体装置に送信してメモリカードに記録させる。その後、ステップS414で、エンタテインメント本体装置に対してプログラム実行許可命令を送信する。

【0119】ユーザデータベース5にディスクIDは存在するが、対応機器IDがデータベース中のものと一致しない場合、ステップS408からステップS410に進み、パ

スワードの入力要求をエンタテインメント本体装置1に送信する。この入力要求は、本体装置1に接続されたテレビジョンモニタ（図示せず。）に表示される。ステップS411で、ユーザから受信したパスワードが、正当か否かが判断される。正当であれば、ステップS412に進み、このディスクの借用者等に新たなパスワードを発行して送信する。ディスク借用者等がディスク所有者からディスクを合意のもとで借りるとき、このパスワードを入力することで、プログラム実行拒否命令を回避することが可能となる。この結果、ディスク借用者は、必ずしもディスク所有者から、ディスク2と共にメモリカード11を借りる必要が無くなる。また、ステップS412では、ディスク所有者に対して発行したディスク固有のパスワードを更新する。更新したパスワードはディスク所有者に対して送信される。これにより中古品の蔓延を助長することが回避できる。

【0120】ステップS412の後、ステップS414で、認証用サーバ4は、エンタテインメント本体装置に対してプログラム実行許可命令を送信する。

【0121】ステップS411で、ユーザから受信したパスワードが正当ではないと判断された場合は、ステップS413に進み、認証用サーバ4からエンタテインメント本体装置に対して、プログラム実行拒否命令が送信される。

【0122】上述した第1のディスクID認証システム及び第2のディスクID認証システムの実施例では、ユーザは、自分のエンタテインメント装置1に対して、手許にある光ディスクのような記録媒体からプログラムを読み込んでいる。しかし、本発明はこれに限定されない。例えば、ディスクIDが付与された記録媒体が他所にあり、遠隔操作により第1又は第2のディスクID認証システムを実行して認証許可を得た後で、その記録媒体に記録されたプログラムをダウンロードすることも出来る。或いは、例えば、ディスクIDが付与された記録媒体が他所にあり、その記録媒体に記録されたプログラムをダウンロードした後で、第1又は第2のディスクID認証システムを実行して認証許可を得て、プログラムを実行することも出来る。

【0123】

【発明の効果】本発明によれば、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムを提供することができる。

【0124】更に、本発明によれば、光ディスク等の記録媒体が不正使用されているか否かを検証する認証システムを有するコンピュータシステムの使用方法を提供することができる。

【図面の簡単な説明】

【図1】図1は、ディスクID認証システムを説明する図である。

【図2】図2は、図1のエンタテインメント本体装置の

構成を示す図である。

【図3】図3は、第1のディスクID認証方法における本体装置側の処理のフローである。

【図4】図4は、第1のディスクID認証方法における認証用サーバ側の処理のフローである。

【図5】図5は、第2のディスクID認証方法における本体装置側の処理のフローである。

【図6】図6は、第2のディスクID認証方法における認証用サーバ側の処理のフローである。

【図7】図7は、認証用サーバが受信したディスクID 10 11：メモ리카ード（第2の記録媒体）

及び機器IDと、ユーザデータベースに予め蓄積されたユーザ情報との比較結果を表す表である。

【符号の説明】

1：エンタテインメント本体装置（コンピュータ）

2：光ディスク（第1の記録媒体）

4：認証用サーバ

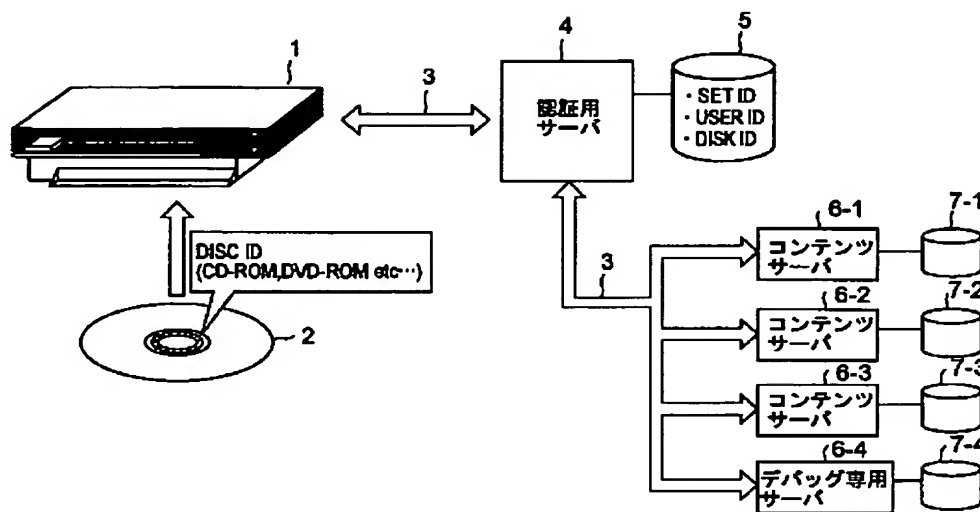
5：ユーザデータベース

6：コンテンツサーバ

7：データベース

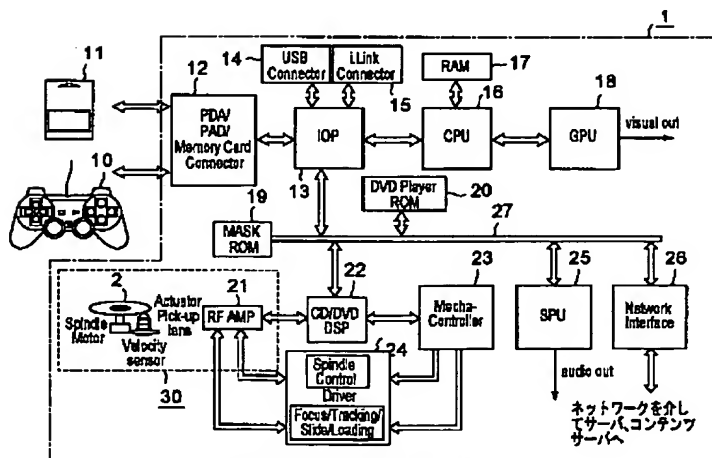
11：メモ리카ード（第2の記録媒体）

【図1】



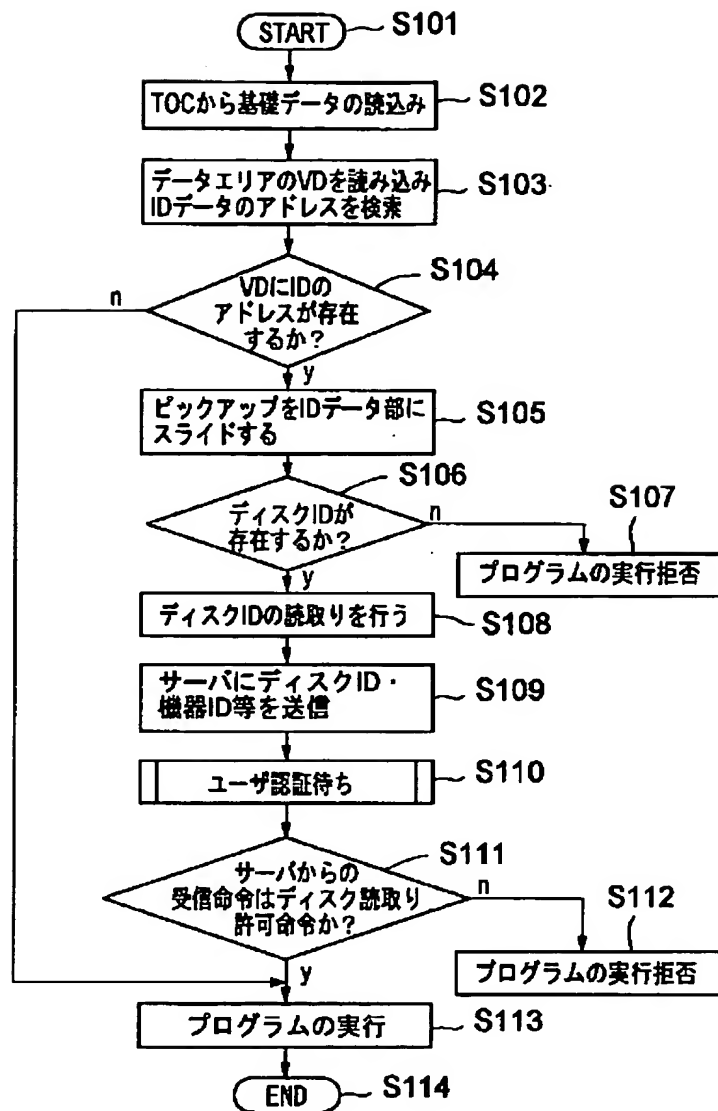
システムの概念図

【図2】



エンタテインメント本体装置の構成

【図3】

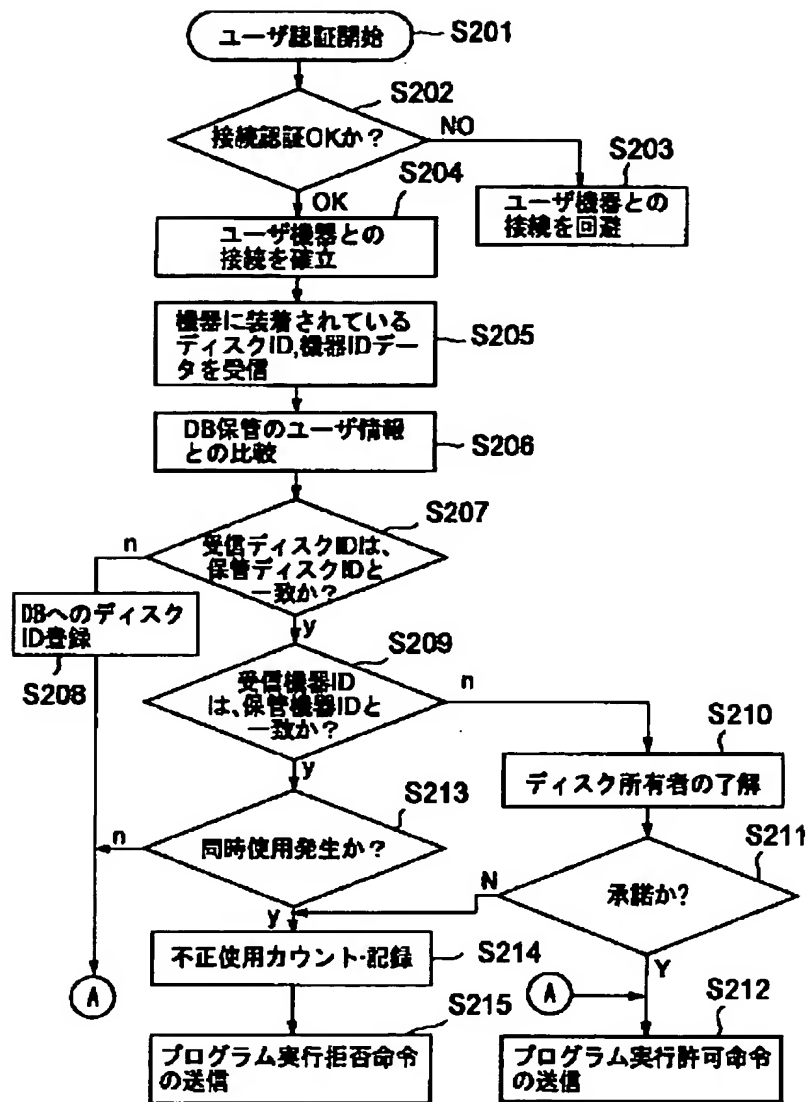


ディスクID認証 (本体装置側処理)

【図7】

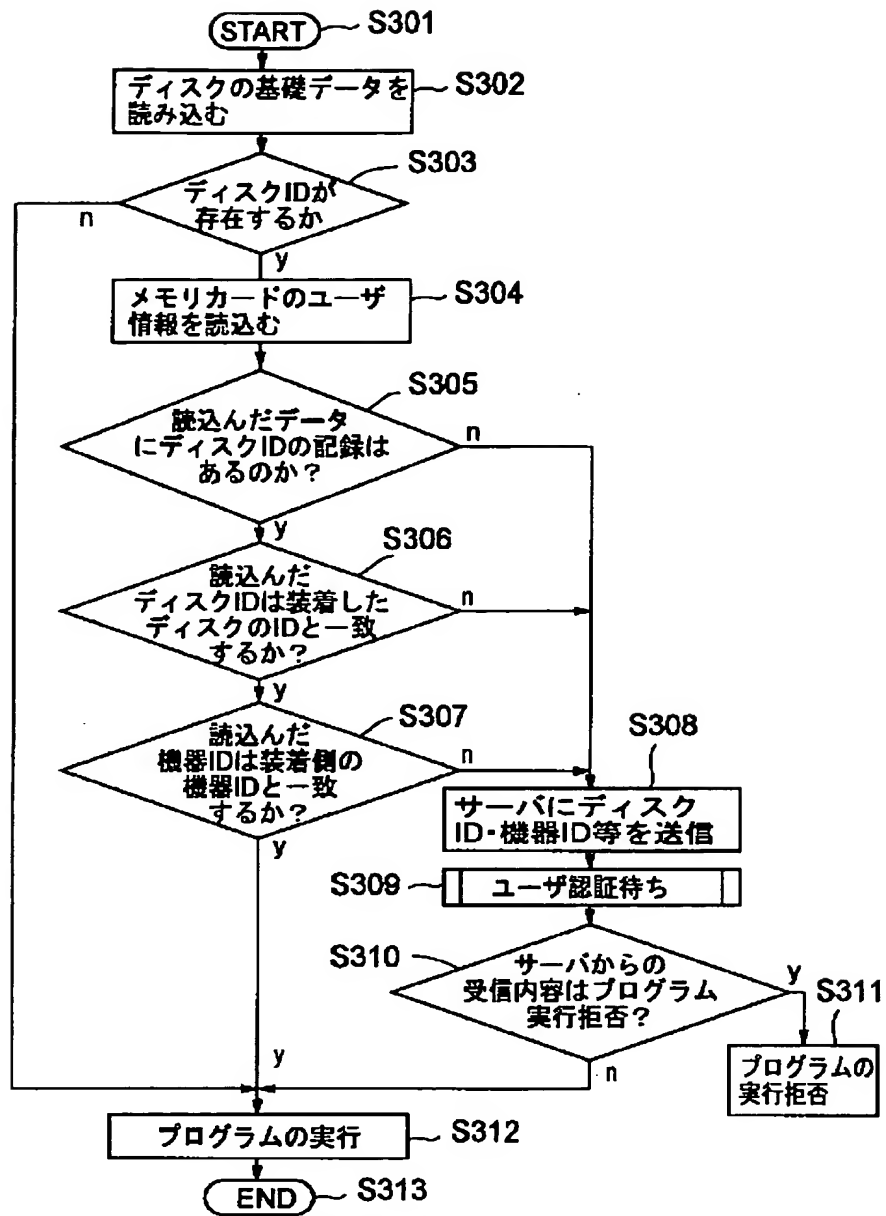
No.	送信情報	蓄積されたディスクID	蓄積された機器ID
1	送信ディスクID, 送信機器ID	○	○
2		○	×
3		×	○
4		×	×

【図4】



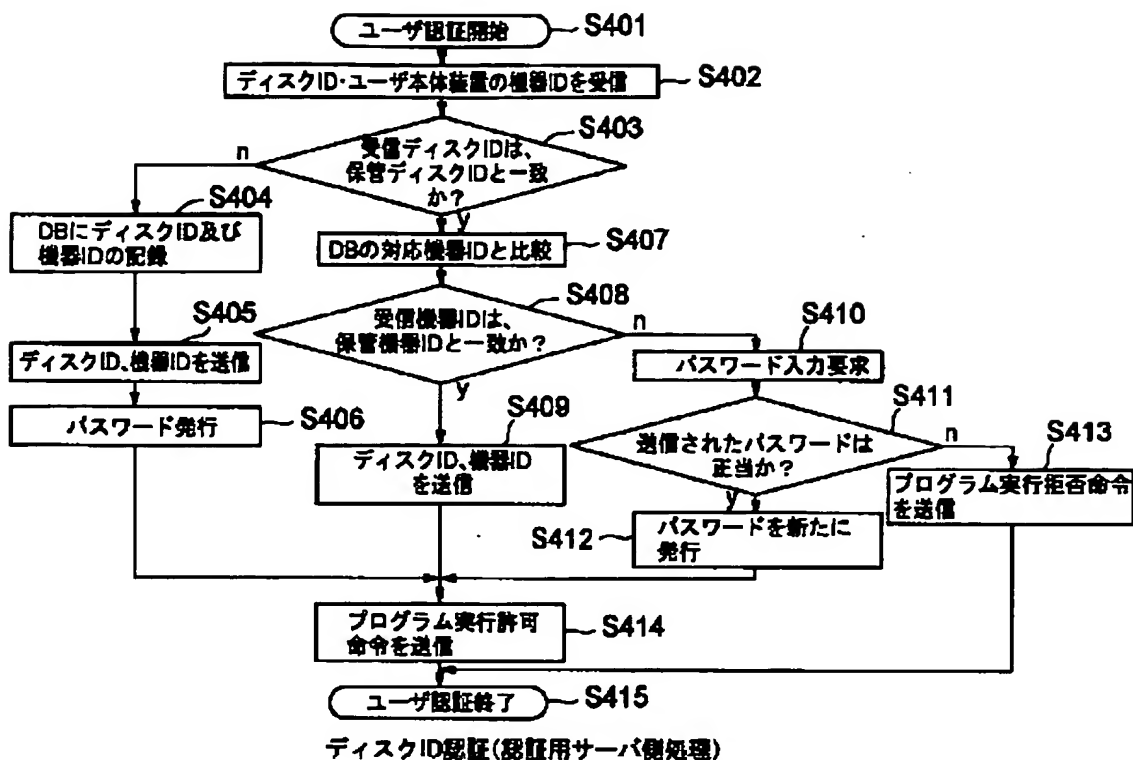
ディスクID認証(認証用サーバー側処理)

【図5】



ディスクID認証(本体側処理)

【図6】



フロントページの続き

(51)Int.Cl.⁷

G 1 1 B 27/00

識別記号

F I

G 1 1 B 27/00

テームコード(参考)

A

(72)発明者 岡本 伸一

東京都港区赤坂7丁目1番1号 株式会社
ソニー・コンピュータエンタテインメント
内

(72)発明者 三浦 和夫

東京都港区赤坂7丁目1番1号 株式会社
ソニー・コンピュータエンタテインメント
内

Fターム(参考) 5B017 AA06 BB09 BB10 CA09 CA16

5B065 BA03 PA00 PA11

5D044 AB02 BC03 CC06 DE48 DE50

DE54 FG18 GK12 HH15 HL02

HL11

5D090 AA01 BB02 CC04 FF24 GG17

GG36

5D110 AA15 BB01 BB24 DA04 DA12

DB03 DC05 DE01 EA07

This Page is inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox